

CLAIMS

1. A method for encoding electronically readable cards having a card surface with visually readable indicia corresponding to an authorized user of said card and an electronically readable digital data storage medium permanently affixed to said card, comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect of the said individual; and

storing one or both of said first reference data element and said second reference data element on either said card data storage medium or in an off-card storage;

whereby confidence in identification of a card user as the said authorized user is substantially increased by verifying the first and said second reference data elements against live data derived at a card transaction site in the course of a card transaction.

2. The method of Claim 1 further comprising the steps of:

applying an encoding algorithm to said first reference data element and said second reference data element thereby to derive an encoded data element; and

recording said encoded data element on said data storage medium for reading by an electronic card reader.

3. The method of Claim 1 wherein said digital data storage medium is a magnetic stripe.

4. The method of Claim 1 wherein said biometric aspect is a fingerprint and said second data element is derived from a scanned image of a finger of the said individual.

5. The method of claim 1 wherein said visually readable indicia include alphanumeric indicia.

6. The method of claim 1 wherein said visually readable indicia include photographic indicia.

7. The method of claim 1 wherein said visually readable indicia include the name and a photograph of the said authorized user of the card.

8. The method of Claim 1 further comprising the step of deriving a third reference data element representative of a scanned image of said indicia and storing said third reference data element on either said card data storage medium or in off-card storage; and verifying said third reference data element against a live third data element derived at a card transaction terminal in the course of a card transaction.

9. The method of Claim 8 further comprising the steps of also applying said encoding algorithm to said third data element with said first and said second data element thereby to factor said third data element in said encoded data element.

10. The method of Claim 1 wherein said step of deriving a first reference data element comprises the steps of scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

11. The method of Claim 1 wherein said step of deriving a second reference data element comprises the steps of applying a live fingerprint to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image.

12. The method of Claim 8 wherein said step of deriving a third reference data element comprises the steps of scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face.

13. A method for verifying the authenticity of a mag-stripe card and verifying the identity of a card user presenting the card at a transaction site, said mag-stripe card having a card surface with visually readable indicia indicative of an authorized user of said card and an electronically readable digital data storage magnetic stripe permanently affixed to said card, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect of the person of said card user;

deriving a third reference data element representative of a scanned image of said visually readable indicia;

applying an encoding algorithm to said first reference data element, said second reference data element and said third reference data element thereby to derive an encoded data element;

recording said encoded data element on said data storage medium for reading by an electronic card reader;

5 comparing at least two of said first, said second and said third reference data elements against corresponding live data elements derived at a card transaction site in the course of a card transaction; and

authorizing a card transaction if said least two of said first, said second and said third reference data elements are validated by said comparing.

10

14. The method of claim 13 wherein said step of verifying comprises the steps of:

providing a card reader at a transaction location;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said magnetic stripe of said mag-stripe card;

15 applying a first decoding algorithm to said encoded data element to retrieve said first reference data element, said second reference data element and said third reference data element;

deriving a first live data element representative of random microstructure in said data storage medium of said mag-stripe card;

20 deriving a second live data element representative of a biometric aspect of the person presenting the card;

deriving a third live data element representative of a scanned image of said visually readable indicia;

25 comparing said first live, said second live and said third live data element against said first reference, said second reference and said third reference data element; and

authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if any said live data element is not so validated.

30 15. The method of claim 14 wherein said card reader comprises a DeLand enabled scanner and said step of deriving a first live data element comprises the steps of scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

16. The method of claim 14 wherein said card reader comprises a fingerprint scanner and said step of deriving a second live data element comprises the steps of applying a live fingerprint to said fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image.

5

17. The method of claim 14 wherein said card reader comprises a card face imager and said step of deriving a third live data element comprises the steps of scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face.

10

18. A method for encoding a mag-stripe card for use in electronic transactions, said mag-stripe card having a card surface with visually readable indicia associated with an authorized user of said card and an electronically readable digital data storage magnetic stripe element permanently affixed to said card, said method comprising the steps of:

15

deriving a first reference data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure;

20

deriving a second reference data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the authorized user of the card to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

25

deriving a third reference data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face;

applying a fourth encoding algorithm to said first reference data element, said second reference data element and said third reference data element thereby to derive an encoded data element; and

recording said encoded data element on said mag-stripe element.

30

///

///

19. A method for verifying the authenticity of a mag-stripe card encoded as in Claim 18 and verifying the identity of a card user presenting said mag-stripe card at a transaction site, comprising the steps of:

providing a mag-stripe card reader at a transaction location, said card reader comprising a

5 DeLand enabled scanner, a fingerprint scanner, and a card face imager;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said mag-stripe element of said mag-stripe card;

applying a first decoding algorithm to said encoded data element to retrieve said first reference data element, said second reference data element and said third reference data

10 element;

deriving a first live data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying said first encoding algorithm to extract and encode features from digitized microstructure;

15 deriving a second live data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the card user to said fingerprint scanner of the card reader at the transaction location, scanning and digitizing an image of said live fingerprint and applying said second encoding algorithm to extract and encode features from the digitized fingerprint image;

20 deriving a third live data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face with said card face imager at the transaction location and applying said third encoding algorithm to extract and encode features from the digitized image of said card face;

comparing said first live, said second live and said third live data element against said first reference, said second reference and said third reference data element; and

25 authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if any said live data element is not so validated.

30 20. A method for improving the security of mag-stripe card based transactions, comprising the steps of:

providing a mag-stripe card having a card surface with visually readable indicia associated with an authorized user of said card and an electronically readable digital data storage magnetic stripe element permanently affixed to said card;

deriving either a first reference data element representative of random microstructure in said magnetic stripe element by scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure or a third reference data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face;

deriving a second reference data element representative of a biometric aspect of the person of said authorized user by applying a live fingerprint of the authorized user of the card to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

applying a fourth encoding algorithm to said first reference data element and said second reference data element to derive an encoded data element;

recording said encoded data element on said mag-stripe element.

providing a mag-stripe card reader at a transaction location, said card reader comprising a scanner enabled for scanning and digitizing microstructure of said magnetic stripe, a fingerprint scanner, and a card face imager;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said mag-stripe element of said mag-stripe card;

applying a first decoding algorithm to said encoded data element to retrieve said either first or third reference data element and said second reference data element;

deriving either a first live data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying said first encoding algorithm to extract and encode features from digitized microstructure or a third live data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face with said card face imager at the transaction location and applying said third encoding algorithm to extract and encode features from the digitized image of said card face;

deriving a second live data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the card user to said fingerprint scanner of the card reader at the transaction location, scanning and digitizing an image of said live fingerprint and applying said second encoding algorithm to extract and encode features from the digitized fingerprint image;

comparing said either first or third live data element against said either first or third reference data element;

comparing said second live data element against said second reference data element;
and

5 authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if either said live data element is not so validated.

10 21. The method of claim 20 wherein said card reader comprising a scanner enabled for scanning and digitizing microstructure of said magnetic stripe is a DeLand enabled card reader.

22. A method for encoding electronically readable mag-stripe cards having a card surface with visually readable indicia corresponding to an authorized user of said card and a magnetic data storage mag-stripe element affixed thereto, comprising the steps of:

15 deriving a card authenticating reference data element representative of either random microstructure in said mag-stripe element or representative of a scanned image of said indicia
deriving a second reference data element representative of a biometric aspect of the authorized user; and

20 applying an encoding algorithm to said card authenticating reference data element and said second reference data element thereby to derive an encoded data element; and

recording said encoded data element on said data storage medium for reading by an electronic card reader at a card transaction location.

23. A method for verifying the authenticity of a mag-stripe card encoded as in Claim 22 and
25 verifying the identity of a card user presenting said mag-stripe card at a transaction site, comprising the steps of retrieving said card authenticating reference data element and said second reference data element by decoding said encoded data element and verifying each said reference data element against a corresponding live data element derived at a card transaction terminal in the course of a card transaction.

30 ///

///